doi:10.11835/j.issn.1000-582X.2017.04.006

基于层次分析法的信息安全风险评估要素量化方法

柴继文[1],王　胜[1],梁晖辉[1],胡　兵[2],向　宏[2]
(1.国网四川省电力公司电力科学研究院,成都 610072;
2.重庆大学　信息物理社会可信服务计算教育部重点实验室,重庆 400044)

摘　要:信息安全风险评估是保障信息系统安全的重要基础性工作,但现有风险评估标准和相关研究提供的评估模型和计算方法的评估结果不能有效体现信息系统资产在保密性、完整性、可用性上的不同安全需求和面临的不同风险。利用层次分析法建立风险评估层次分析模型,在借鉴通用脆弱性评分系统指标评价体系基础上改进脆弱性要素量化方法,利用构建的层次分析模型偏量判断矩阵计算"安全事件损失""安全事件可能性"和"风险值"。通过实验验证,与现有方法相比,所提方法的评估结果能够直观体现资产在保密性、完整性和可用性上面临的不同风险,能为制定风险控制措施提供更加准确、合理的建议。

关键词:风险评估;层次分析法;脆弱性;偏量判断矩阵
中图分类号:TP309　　**文献标志码**:A　　**文章编号**:1000-582X(2017)04-044-10

An AHP-based quantified method of information security risk assessment elements

CHAI Jiwen[1], *WANG Sheng*[1], *LIANG Huihui*[1], *HU Bing*[2], *XIANG Hong*[2]
(1. State Gid Sichuan Electric Power Research Institute, Chengdu 610072, P.R.China;
2. Key Laboratory of Dependable Service Computing in Cyber Physical Society, Ministry of Education, Chongqing University, Chongqing 400044, P.R.China)

Abstract: Information security risk assessment is an important foundation work for security protection of information systems, but the assessment results of the existing risk assessment criteria and related research models and calculation methods cannot effectively reflect different security needs and risks of the confidentiality, the integrity and the availability of information system assets. In this paper, we used analytic hierarchy process (AHP) to establish a risk assessment analytic hierarchy process model first, then improved vulnerability factor quantitative methods based on the common vulnerability scoring system evaluation index system, and finally used the model's deviator judgment matrix to compute "security incident loss", "security event possibility" and "value-at-risk". Experiment results show the proposed method can more intuitively reflect different risks of the confidentiality, the integrity and the availability of assets than conventional methods, and it can provide more accurate and reasonable recommendations for the development of risk control measures.

Keywords: risk assessment; analytic hierarchy process; vulnerability; deviator judgment matrix

---

收稿日期:2016-09-05
基金项目:国网四川省电力公司科技项目(5219991351VR);国家自然科学基金资助项目(61472054)。
Supported by Science and Technology Project of State Gid Sichuan Electric Power Research Institute (5219991351VR) and National Natural Science Foundation of China(61472054).
作者简介:柴继文(1963-),男,国网四川省电力公司电力科学研究院副总工程师,高级工程师。
向宏(联系人),男,重庆大学教授,博士生导师,(E-mail) xianghong@cqu.edu.cn。

信息安全风险评估是信息安全保障工作的基础性工作和重要环节[1]，为信息安全保障体系的建设提供必需的决策依据。信息系统的风险评估可以描述为威胁（外因）利用脆弱性（内因）对资产（主体）产生影响的评价过程。作为威胁与资产的关联要素，对脆弱性的评价应该包括被威胁利用的难易程度和被利用后对资产的损害程度两个方面，以保证参与这一过程的外因、内因和主体互不干扰；同时需要考虑信息系统资产在保密性、完整性、可用性方面的不同安全需求，以保证最终评价结果的科学性和准确性。

现有信息安全风险评估流程主要依据 NIST SP 800-30[2] 和 GB/T 20984—2007[1] 进行实施。在现有标准基础上对风险评估的研究工作主要集中在以下两个方面：一是对风险评估标准[1] 所提出的模型进行优化改进，主要采用模糊分析法和层次分析法，如文献[3]利用层次分析法[4] 建立安全风险定量评估应用模型，运用灰色理论及熵权系数法[5] 减少风险计算中主观因素的影响，文献[6]基于模糊综合评判决策模型[7] 计算风险事件发生的可能性模型，并采用层次分析法构建比较判断矩阵计算风险影响的大小，文献[8]通过对资产、威胁、脆弱性等风险要素的层次化分析，提出一种层次化风险评估方法来量化风险，该方法将安全风险分为组件级、系统级和组织级 3 个层面，通过对 3 个层次风险的逐层分析，使得风险分析结果可以更为客观地反映风险评估的层次化需求；二是对参与风险计算的各个要素的量化方法进行研究，如文献[9]根据通用弱点评价体系（CVSS）[10] 的计算方法，从基本度量组、时间度量组和环境度量组 3 个方面对脆弱性要素进行量化计算，文献[11]基于攻击图[12,15-16]和 CVSS 提出了攻击图中脆弱性节点利用概率的计算方法。但上述标准和方法均是依据信息系统资产、脆弱性和威胁各要素最终赋值结果进行风险计算，这一评估过程掩盖了资产要素对保密性、完整性和可用性的不同需求，最终评估结果不能有效体现资产在保密性、完整性和可用性方面所面临的不同风险；同时也导致参与计算的脆弱性要素存在重复计算，对最终结果造成干扰，如脆弱性严重程度包括对资产的损害程度和被利用的难易程度两个方面，而对资产的损害程度参与了安全事件可能性的计算，被利用的难易程度参与了安全事件损失的计算。

基于上述两方面的考虑，采用层次分析法（analytic hierarchy process，AHP）[4] 对现有风险评估模型进行分层细化，避免要素识别的相互干扰，利用各个要素的属性值直接参与计算，构建偏量判断矩阵，使得最终的评估结果能够体现被评估对象在保密性、完整性和可用性上大的不同偏向需求，为信息安全保障工作提供客观、准确的决策依据。

1　风险评估层次分析模型

如图 1 所示，风险评估层次分析模型包括目标层、准则层和指标层。目标层为模型顶层，包含“风险指数”一个元素，该元素取值由准则层所确定；准则层包含“安全事件可能性”和“安全事件损失”，其取值由指标层各要素的属性所确定；指标层是准则层的目标所需的方案，为准则层提供服务。

根据上述层次分析模型，信息系统的风险评估流程如下：

1）对指标层各个要素的属性进行识别和赋值，包括：资产要素属性的识别及量化；脆弱性要素属性的识别及量化，脆弱性要素属性包括“对资产的损害程度”和“被利用难易程度”两个方面；威胁要素的识别及量化；安全措施要素的识别及量化。

2）根据资产要素和脆弱性要素中“对资产的损害程度”属性的量化结果，计算安全事件损失。

3）根据安全措施要素、威胁要素和脆弱性要素中“被利用难易程度”属性的量化结果，计算安全事件可能性。

4）根据安全事件损失和安全事件可能性计算资产在保密性、完整性、可用性方面所面临的风险。

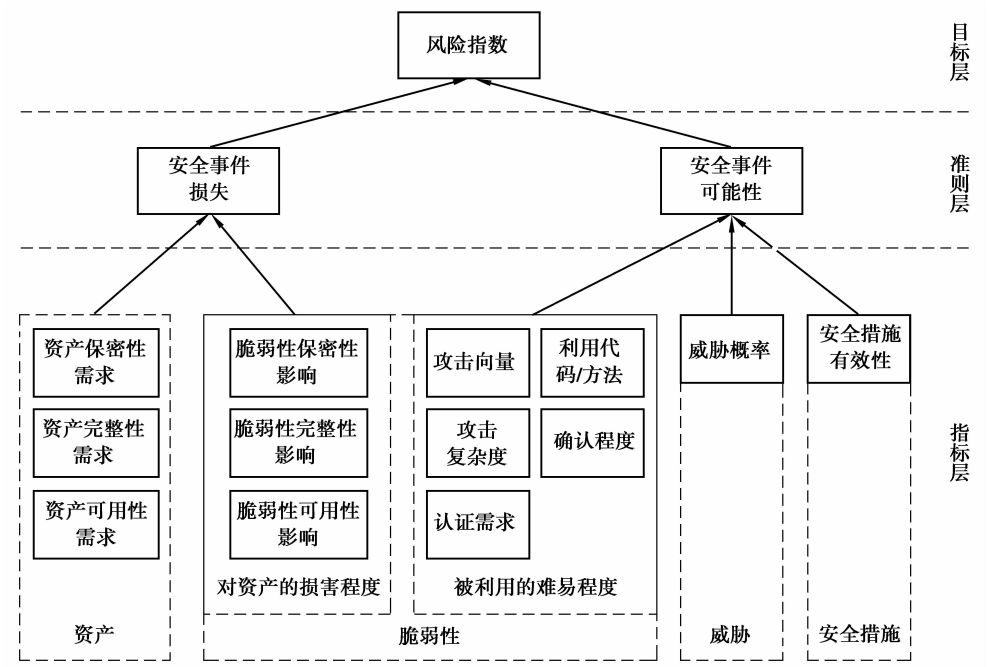

图 1 风险评估层次分析模型

Fig.1 Analytic hierarchy model of risk assessment

2 模型要素量化

2.1 关键要素定义

根据风险评估层次分析模型，对指标层和准则层各要素进行如下定义：

1)定义信息系统资产为 A，在保密性、完整性、可用性 3 个安全属性上的不同需求为其偏量需求，定义为 $(AC|AI|AA)\in A$；

2)定义资产脆弱性为 V，对 V 的评价包括“对资产的损害程度”和“被利用的难易程度”两个方面[1]，“对资产的损害程度”实质是对资产 AC、AI、AA 偏量需求的潜在偏量损害，定义为 $(VC|VI|VA)\in VD$，“被利用的难易程度”定义为 VU；

3)定义信息系统的潜在威胁发生概率为 T，采取的安全措施有效性为 SE；

4)定义安全事件损失为 F，其值由 A 的偏量需求和对应的偏量损害所确定，为 $3\times n$ 的矩阵，定义为偏量损失矩阵，其中 n 为某一资产所存在的脆弱性数量；

5)定义安全事件可能性为 L，其值由脆弱性被利用的难易程度和威胁的概率所确定，为 $n\times k$ 的矩阵，其中 k 为某一资产所面临安全威胁种类的数量；

6)定义风险为 R，其值由 F 和 L 所确定，为 $3\times n$ 的矩阵。

2.2 资产要素量化

信息系统资产(A)的保密性(AC)、完整性(AI)、可用性(AA)是公认的评价资产的 3 个安全属性[1]。对资产 3 个属性的量化赋值不仅需要考虑资产本身的安全需求和所属信息系统的安全特性，还需要考虑其所承载业务应用的重要性和对其他资产的关联影响。文献[1]中对信息系统资产的量化进行了较为科学的定义，因此，借鉴文献[1]的资产识别及量化方法，对资产的保密性、完整性、可用性进行以下的量化赋值，参见表 1。

表 1　资产属性量化值

Table 1　The value of asset attributes

标识	很高	高	中等	低	很低
保密性(C)	5	4	3	2	1
完整性(I)	5	4	3	2	1
可用性(A)	5	4	3	2	1

2.3　脆弱性要素量化

对脆弱性(V)的识别基本采用工具检测和人工测评的方法,对其量化基本采用通用脆弱性评分系统(common vulnerability scoring system, CVSS)的计算方法。CVSS 从基本度量(base metrics)、生命周期度量(temporal metrics)和环境度量(environmental metrics)3 个方面评价脆弱性[5]。基本度量包括攻击向量(AV)、攻击复杂度(AC)、所需权限(PR)、保密性影响(VC)、完整性影响(VI)、可用性影响(VA)等指标,生命周期度量包括利用可能性(E)、可修复等级(RL)和脆弱性报告确认程度(RC),环境度量包括安全需求(CR、IR、AR)和可修改的基本指标(MAV、MAC、MPR、MC、MI、MA)。

依据本文的风险评估层次分析模型,上述指标中生命周期度量的 RL 指标可在安全措施要素量化中考虑,环境度量的安全需求指标已在资产要素量化中考虑,可修改的指标在基本度量指标的量化中考虑。同时考虑脆弱性要素属性包括“对资产的损害程度”和“被利用难易程度”,需要从损害程度度量(VD)和利用难易程度度量(VU)两个方面对 $CVSS$ 现有度量指标进行重新分类,其量化规则参见表 2,3[5],其中:

$$VD = 10.41 \times (1 - (1 - VC) \times (1 - VI) \times (1 - VA)),$$

$$VU = 20 \times AV \times AC \times PR \times E \times RC。$$

表 2　漏洞损害程度度量

Table 2　The damage degree of vulnerability

度量因素	类型	赋值
保密性影响(VC)	无影响	0
	部分影响	0.275
	完全影响	0.660
完整性影响(VI)	无影响	0
	部分影响	0.275
	完全影响	0.660
可用性影响(VA)	无影响	0
	部分影响	0.275
	完全影响	0.660

表 3　漏洞利用难易程度度量

Table 3　The exploit difficulty of vulnerability

度量因素	类型	赋值
攻击向量(AV)	本地	0.395
	邻近网络	0.646
	远程	1.0

续表

度量因素	类型	赋值
攻击复杂度(AC)	高	0.35
	中	0.61
	低	0.71
所需权限(PR)	需要多重身份验证	0.45
	需要单重身份验证	0.56
	不需要	0.74
利用可能性(E)	未证明	0.85
	理论证明	0.9
	实际可以	0.95
	高利用性	1.0
脆弱性报告确认程度(RC)	未定义	1.0
	未确认	0.9
	未证实	0.95
	已确认	1.0
	未定义	1.0

2.4 威胁要素量化

威胁(T)识别需要首先对威胁的来源进行确认,并对各个来源的威胁进行分类,通过对各来源威胁种类出现的频率进行统计以便对威胁进行量化。威胁的来源及其分类可参照《信息安全技术—信息安全风险评估规范》[1],威胁量化值参见表4。

表4 威胁属性量化值

Table 4 The value of threat

标识	很高	高	中等	低	很低
威胁频率	5	4	3	2	1

2.5 安全措施要素量化

安全措施(SE)的识别需要通过实际调研确认信息系统所采取的各项安全防护措施,并验证采取的安全防护措施对各类威胁进行防护的有效性。参照《涉及国家秘密的信息系统分级保护测评指南》的相关规则[14]定义安全措施的量化规则,见表5。

表5 安全措施量化

Table 5 The value of security measure

等级	标识	定义
1	有效	所采取的安全防护措施能够有效阻止威胁的发生
0.6	基本有效	所采取的安全防护措施能减少威胁的发生,但防护不全面
0	无效	未采取相应安全防护措施,或所采取的措施无效

2.6　安全事件损失量化计算

安全事件的损失由资产的价值和脆弱性的损害程度所决定，为避免计算结果掩盖资产对 C、I、A 属性的偏向需求，应该以资产(A)价值的 AC、AI、AA 属性和脆弱性(V)损害程度(VD)的 VC、VI、VA 属性直接运算，得到安全事件损失判断矩阵。

假设信息系统共有 m 个资产，第 x 个资产 A_x 的保密性、完整性、可用性赋值为 AC_x、AI_x、AA_x，该资产有 n 个脆弱性，第 y 个脆弱性 V_y 的损害程度 VD_y 赋值为 VC_x、VI_x、VA_x，则资产 A_x 所存在的 n 个脆弱性对其潜在的损害程度按照以下步骤和公式进行计算。

1)依次计算 n 个脆弱性各自对资产 A_x 的偏量损失，公式(1)为第 y 个脆弱性 V_y 对资产 A_x 的偏量损失矩阵。

$$f_y = f(A_x \mid VD_y) = (AC_x \mid AI_x \mid AA_x)^{\mathrm{T}} \times (VC_y \mid VI_y \mid BA_y) \times$$
$$(1 \mid 1 \mid 1)^{\mathrm{T}} = \begin{bmatrix} AC_xVC_y \\ AI_xVI_y \\ AA_xVA_y \end{bmatrix}_{3\times 1}, \begin{pmatrix} 1 \leqslant x \leqslant m \\ 1 \leqslant y \leqslant n \end{pmatrix}。 \tag{1}$$

2)利用公式(1)的计算结果构造 n 个脆弱性对资产 A_x 造成损害的总体偏量损失矩阵，见式(2)，式中每一列为 V_y 对资产 A_x 的损害偏量，其值参见式(1)、(3)、(4)、(5)。

$$F_x = F(f_y) = \begin{pmatrix} fC_1 \cdots fC_y \cdots fC_n \\ fI_1 \cdots fI_y \cdots fI_n \\ fA_1 \cdots fA_y \cdots fA_n \end{pmatrix}_{3\times n}, \tag{2}$$

$$fC_y = AC_xVC_y, \begin{pmatrix} 1 \leqslant x \leqslant m \\ 1 \leqslant y \leqslant n \end{pmatrix}; \tag{3}$$

$$fI_y = AI_xVI_y, \begin{pmatrix} 1 \leqslant x \leqslant m \\ 1 \leqslant y \leqslant n \end{pmatrix}; \tag{4}$$

$$fA_y = AA_xVA_y, \begin{pmatrix} 1 \leqslant x \leqslant m \\ 1 \leqslant y \leqslant n \end{pmatrix}。 \tag{5}$$

2.7　安全事件可能性量化计算

安全事件可能性由脆弱性的被利用难易程度、对应威胁发生的概率，以及针对该威胁所采取的安全防护措施所决定的。

假设信息系统第 x 个资产 A_x 面临 K 个威胁，采取了 K 项安全防护措施，则资产 A_x 所面临的 K 个安全威胁利用 A_x 所存在的 n 个脆弱性转化为安全事件的可能性按照以下步骤和公式进行计算。

$$L_x = l(VU \mid T'), (1 \leqslant x \leqslant m), \tag{6}$$
$$VU_y = AV_y \times AC_y \times PR_y \times E_y \times RC_y, \tag{7}$$
$$T'_z = T_z \times (1 - SE_z)。 \tag{8}$$

式(6)中 VU 为脆弱性的被利用难易程度，T'为采取安全防护措施后威胁的概率，式(7)计算第 y 个脆弱性 V_y 的被利用难易程度，式(8)计算第 z 个威胁 T_z 在采取安全防护措施后的概率，SE 为所采取安全防护措施的有效性。将式(7)、式(8)代入式(6)中，得到 K 个安全威胁利用 A_x 的 n 个脆弱性转化为安全事件的可能性判断矩阵，参见式(9)，式中第 y 行表示 K 个安全威胁利用 V_y 转换成安全事件的可能性，式中第 z 列表示 T_z 利用 n 个脆弱性转换成安全事件的可能性。

$$\boldsymbol{L}_x = (VU_1 \mid \cdots \mid VU_y \mid \cdots \mid VU_n)^{\mathrm{T}} \times (T'_1 \mid \cdots \mid T'_z \mid \cdots \mid T'_k) =$$
$$\begin{pmatrix} VU_1T'_1 \cdots VU_1T'_z \cdots VU_1T'_k \\ VU_2T'_1 \cdots VU_2T'_z \cdots VU_2T'_k \\ \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \\ VU_yT'_1 \cdots VU_yT'_z \cdots VU_yT'_k \\ VU_nT'_1 \cdots VU_nT'_z \cdots VU_nT'_k \end{pmatrix}_{n\times k}, \begin{pmatrix} (1 \leqslant x \leqslant m \\ 1 \leqslant y \leqslant n \\ 1 \leqslant z \leqslant k) \end{pmatrix}。 \tag{9}$$

2.8 风险值量化计算

信息系统资产 A_x 的风险 R_x 由安全事件损失 F_x 和安全事件可能 L_x 所确定，采用式(10)进行计算，式中每一列为 T_z 利用资产 A_x 所存在的 n 个脆弱性对 A_x 的保密性、完整性、可用性所造成的风险影响，其值参见式(11)-(13)。

$$R_x=(F_x \mid L_x)=\begin{pmatrix} fC1\cdots fC_y\cdots fC_n \\ fI1\cdots fI_y\cdots fI_n \\ fA1\cdots fA_y\cdots fA_n \end{pmatrix}_{3\times n} \times \begin{pmatrix} VU_1T'_1\cdots VU_1T'_z\cdots VU_1T'_k \\ VU_2T'_1\cdots VU_2T'_z\cdots VU_2T'_k \\ \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \\ VU_yT'_1\cdots VU_yT'_z\cdots VU_yT'_k \\ VU_nT'_1\cdots VU_nT'_z\cdots VU_nT'_k \end{pmatrix}_{n\times k} =$$

$$\begin{pmatrix} rC_1\ rC_2\ \cdots\ rC_z\ \cdots\ rC_k \\ rI_1\ rI_2\ \cdots\ rI_z\ \cdots\ rI_k \\ rA_1\ rA_2\ \cdots\ rA_z\ \cdots\ rC_k \end{pmatrix}_{3\times k}, \begin{pmatrix} 1\leqslant x\leqslant m \\ 1\leqslant y\leqslant n \\ 1\leqslant z\leqslant k \end{pmatrix}, \tag{10}$$

$$rC_z=AC_xT'_z\sum_{y=1}^{n}VC_yVU_y, \tag{11}$$

$$rI_z=AI_xT'_z\sum_{y=1}^{n}VI_yVU_y, \tag{12}$$

$$rA_z=AA_xT'_z\sum_{y=1}^{n}VA_yVU_y。 \tag{13}$$

3 实验分析

为验证本文所提出模型的科学性和计算方法的可靠性，选取文献[13]“兰芯”子系统中编号为“D_A01”资产的风险评估结果和分析结论进行对比验证。

在文献[13]中“D_A01”为“兰芯”子系统的应用服务器，安装 aix5.3 操作系统，存在 5 个脆弱性，面临来自“信息载体故障、信息环境、无合作的外部人员、合作的第三方人员、无意思破坏内部人员、有意识破坏内部人员”[13] 6 个方面的潜在威胁。表 6-8 为文献[13]对“D_A01”资产、脆弱性和威胁的赋值结果，表 9 为文献[3]根据文献[13]的计算方法对“D_A01”进行风险计算的结果。

表 6 文献[13]资产赋值结果

Table 6 The asset evaluation results in literature [13]

编 号	保密性	完整性	可用性	资产价值
D_A01	4	5	5	5

表 7 文献[13]脆弱性赋值结果

Table 7 The vulnerability evaluation results in literature [13]

编 号	脆弱性编号	脆弱性赋值
v_1	CVE-2004-0786	4
v_2	CVE-2004-0747	4
v_3	CVE-2004-0751	4
v_4	CVE-2004-0748	4
v_5	CVE-2004-0809	4

表 8　文献[13]威胁频率赋值结果

Table 8　The threat evaluation results in literature [13]

编　号	威胁源	赋值
T_1	信息载体故障	4
T_2	信息环境	1
T_3	无合作的外部人员	5
T_4	合作的第三方人员	4
T_5	无意识破坏内部人员	4
T_6	有意识破坏内部人员	5

表 9　文献[3]风险计算结果

Table 9　The risk assessment results in literature [3]

编　号	资产	威胁	脆弱性	风险值	风险等级
D_A01	5	23	4	6	高

采用本文风险评估层次分析模型对“D_A01”进行风险计算时,首先需要根据本文 2.3 节的量化方法从“对资产的损害程度(*VD*)”和“被利用难易程度(*VU*)”两个方面对“D_A01”存在的脆弱性进行重新计算,计算结果参见表 10、表 11。

表 10　*VD* 计算结果

Table 10　The assessment results for *VD*

编号	*VC*	*VI*	*VA*	*VD*
v_1	0	0	0.275	2.863
v_2	0.275	0.275	0.275	6.443
v_3	0	0	0.275	2.863
v_4	0	0	0.275	2.863
v_5	0	0	0.275	2.863

表 11　*VU* 计算结果

Table 11　The assessment results for *VU*

编号	*AV*	*AC*	*PR*	*E*	*RC*	*VU*
v_1	1	0.71	0.74	1.0	1.0	10.508
v_2	0.395	0.71	0.74	1.0	1.0	4.151
v_3	1	0.71	0.74	1.0	1.0	10.508
v_4	1	0.71	0.74	1.0	1.0	10.508
v_5	1	0.71	0.74	1.0	1.0	10.508

根据表6、表8、表10、表11的指标量化计算结果，采用本文2.6-2.7节的方法计算安全事件损失(F)、安全事件可能性(L)，以及最终的风险值(R)。由于文献[13]没有对安全措施的有效性进行评估，为便于结果的对比，因此，本文在计算时将安全措施做无效处理，安全措施取值为0，结算结果参见表12-14。

表12 安全事件损失计算结果

Table 12 The assessment results for *F*

F	v_1	v_2	v_3	v_4	v_5
F_C	0	1.1	0	0	0
F_I	0	1.375	0	0	0
F_A	1.1	1.375	1.1	1.1	1.1

表13 安全事件可能性计算结果

Table 13 The assessment results for *L*

L	T_1	T_2	T_3	T_4	T_5	T_6
L_1	42.0	10.5	52.5	42.0	42.0	52.5
L_2	16.6	4.2	20.8	16.6	16.6	20.8
L_3	42.0	10.5	52.5	42.0	42.0	52.5
L_4	42.0	10.5	52.5	42.0	42.0	52.5
L_5	42.0	10.5	52.5	42.0	42.0	52.5

表14 风险值计算结果

Table 14 The assessment results for risk

R	T_1	T_2	T_3	T_4	T_5	T_6
R_C	18.3	4.6	22.8	18.3	18.3	22.8
R_I	22.8	5.7	28.5	22.8	22.8	28.5
R_A	207.8	17.3	259.7	207.8	207.8	259.7

对比表9与表14的风险值计算结果，表14的计算结果则可以直观地分析出“D_A01”资产在可用性方面面临较高的风险，且来源于“无合作的外部人员、有意识破坏内部人员”的威胁在利用“D_A01”所存在的脆弱性后将导致“D_A01”面临很高风险，在对“D_A01”面临的风险进行控制时，所采取的安全防护措施应优先考虑对“D_A01”可用性的保护，并重点防护来源于“无合作的外部人员、有意识破坏内部人员”的威胁；而表9仅能告知“D_A01”资产面临的风险很高，无法对后期采取风险控制措施提供准确、合理的建议。

4 结 语

利用层次分析法对现有信息安全风险评估模型进行分层细化，构建了风险评估层次分析模型。参照通用脆弱性评分系统的指标量化和权值计算方法，改进现行风险评估标准中各要素的识别和量化计算方法，减少参与风险计算各要素之间的耦合性；通过构建偏量判断矩阵，使定量的评估结果能够直观地体现信息系统资产保密性、完整性和可用性所面临的不同风险。采用本文模型和计算方法所得到的资产风险评估结果，可以为后期的风险控制提供更加准确、合理的建议。

参考文献：

[1] 中华人民共和国国家质量监督检查检疫总局，中国国家标准化管理委员会.信息安全技术信息安全风险评估规范：GB/T20984—2007[S].

[2] Stonebumer G, Goguen A, Feringa A. Risk management guide for information technology systems:NIST SP 800-30[S/OL]. [2015-04-16]. http://download.csdn.net/detail/y_t_hon/4977663.

[3] 王莺洁，杜伟娜，罗为.一个灰色信息安全风险评估应用模型[J].通信技术，2010，12(43)：126-128.
WANG Yingjie, DU Weina, LUO Wei. A grey risk assessment model for practical information security[J]. Communications Technology, 2010, 12(43): 126-128. (in Chinese)

[4] Wang Y M, Luo Y, Hua Z. On the extent analysis method for fuzzy AHP and its applications[J]. European Journal of Operational Research, 2008, 186(2): 735-747.

[5] Zhao D M, Wang J H, Wu J, et al. Using fuzzy logic and entropy theory to risk assessment of the information security[C]// International Conference on Machine Learning and Cybernetics. [S.l.]: IEEE, 2005: 2448-2453.

[6] 黄芳芳.信息安全风险评估量化模型的研究与应用[D].武汉：湖北工业大学，2010.
HUANG Fangfang. Research and application for the quantitative model of information security risk assessment[D]. Wuhan: Hubei University of Technology, 2010. (in Chinese)

[7] Chen S H. Operations on fuzzy numbers with function principal[J]. Journal of Management Science, 1985, 6(1): 13-21.

[8] 佟鑫，张利，闵京华.层次化的信息系统风险评估方法研究[J].信息安全与通信保密，2012(8)：59-61.
TONG Xin, ZHANG Li, MIN Jinghua. Study oil hierarchical information system risk assessment[J]. Information And Communication Security, 2012(8): 59-61. (in Chinese)

[10] P Mell, K Scarfone, S Romanosky. A complete guide to the common vulnerability scoring system (CVSS), version 2.0, forum of incident response and security teams[EB/OL]. [2015-04-16]. www.first.org/cvss.

[11] 叶云，徐锡山，齐治昌.大规模网络中攻击图的节点概率计算方法[J].计算机应用与软件，2011，28(11)：136-139.
YE Yun, XU Xishan, QI Zhichang. Attack graph's nodes probabilistic computing approach in a large-scale network[J]. Computer Applications and Software, 2011, 28(11): 137-192. (in Chinese)

[12] Phillips C, Swiler L P. A graph-based system for network-vulnerability analysis[J]. Proceedings of the Workshop on New Security Paradigms, 1998: 71-79.

[13] 向宏，傅鹂，詹榜华.信息安全测评与风险评估.[M].2 版.北京：电子工业出版社，2014.
XIANG Hong, FU Peng, ZHAN Banghua. Information security assessment and risk assessment[M].2nd ed. Beijing: Publishing House of Electronics Industry, 2014. (in Chinese)

[14] 国家保密局.涉及国家秘密的信息系统分级保护测评指南：BMB22—2007[S].

[15] Ingols K, Chu M, Lippmann R, et al. Modeling modern network attacks and countermeasures using attack graphs[C]// Annual Computer Security Applications Conference, Hawaii, USA. [S.l.]: IEEE, 2009:117-126.

[16] Noel S, Elder M, Jajodia S, et al. Topological vulnerability analysis[J]//Springer Berlin Heidelberg, 2005, 3685: 124-129.

（编辑　王维朗）